Secure Identity Research Group
http://www.inf.fu-berlin.de/groups/ag-si/

Freie Universität Berlin

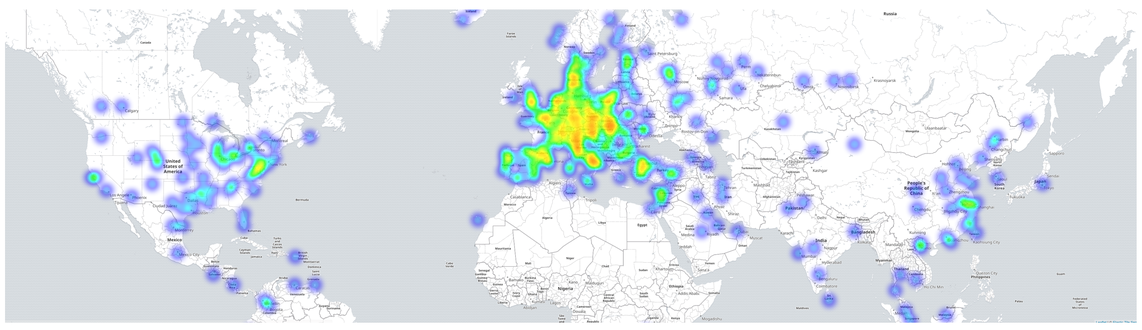
Towards Highly Interactive Honeypots for Industrial Control Systems

Stephan Lau, Johannes Klick, Stephan Arndt and Volker Roth

<firstname>.<surname>@fu-berlin.de

Internet-facing Siemens PLCs

About *3700 Siemens S7 PLCs* are connected to the Internet, at least *230 honeypots* can be trivially identified. Adversaries are likely aware of their existence and may perform a thorough inspections to avoid them. We should improve ICS honeypots regarding their interactivity in order to use them effectively.



Honeypot Classification in the ICS World

Unlike usual honeypots, which only emulate a specific software, Industrial Control Systems are general computing devices. They allow interaction with the system and its loaded program separately. We extended the traditional honeypot classification to account for that:

Low-interactive

The adversary can interact with *the host only*.

Medium-interactive

The adversary can interact with *the host and the program*.

High-interactive

The adversary can additionally *read and write programs*.

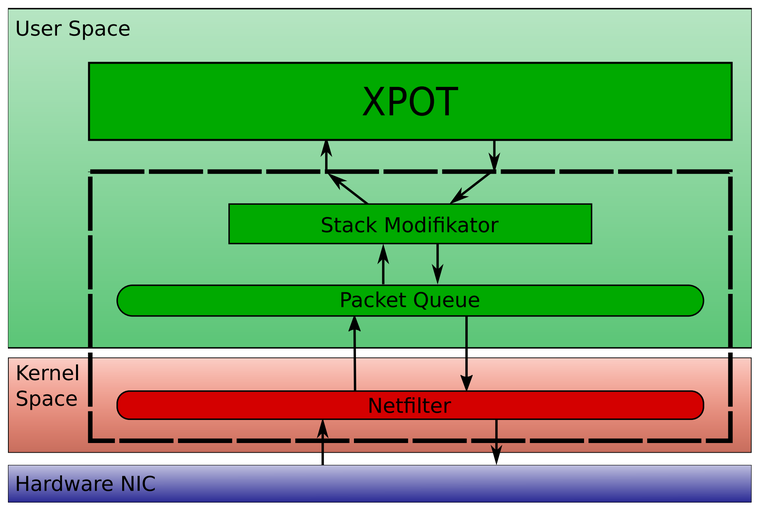
The First High-interactive ICS Honeypot

XPOT is the first high-interactive PLC honeypot and can be used to distract and analyze advanced adversaries. Since it is software-based, it is very scalable and enables large decoy or sensor networks. XPOT can be connected to a simulated industrial process in order to make adversaries' experiences comprehensive.

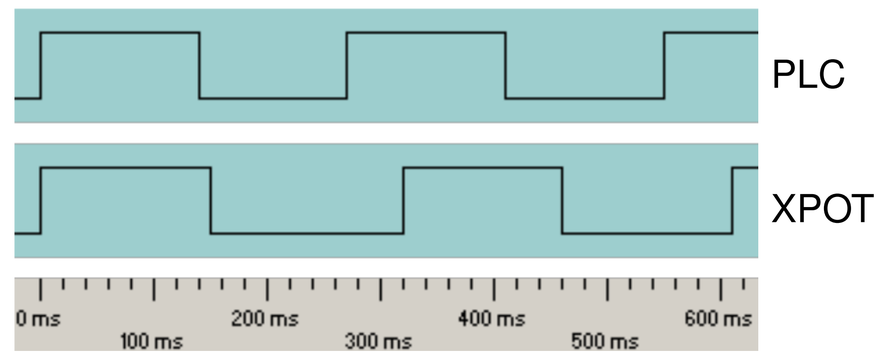
XPOT – A Programmable PLC Honeypot

We developed XPOT, a software-based high-interactive PLC honeypot which can run programs. It simulates a Siemens S7-314C-2 PN/DP.

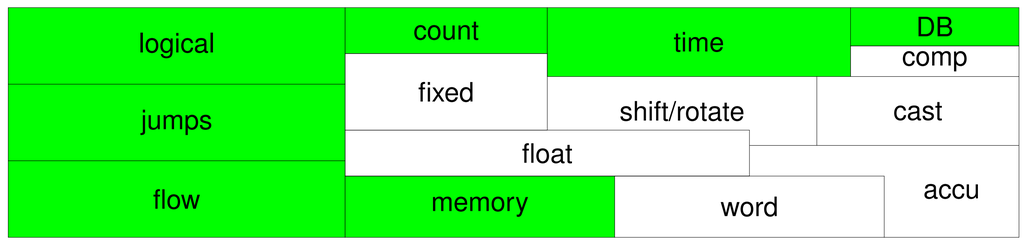
- **modifiable** memory areas
- **debuggable** with monitor mode
- **programmable** with common IDEs
- **executes program**, supports compilation and interpretation
- **spoofed TCP/IP stack**, mimics OS fingerprint and quirks



- **execution time** is close to a genuine PLC



- **most instructions** are supported (100 out of 146)



Features and Classification of ICS Honeypots

	less-interactive			medium-interactive				high-interactive	
	TCP/IP stack spoofing	read System State List	HTTP SNMP	list blocks	read memory	write memory	start/stop CPU	up-/download blocks	execute program
Conpot	–	✓	–	–	–	–	–	–	–
Snap7	–	✓	–	(✓)	(✓)	(✓)	(✓)	–	–
CryPLH2	(✓)	✓	✓	✓	✓	✓	✓	✓	–
XPOT	✓	✓	SNMP	✓	✓	✓	✓	✓	✓